Introduction to Malware Forensics (WBT)

Self-paced online training

This online course explains how to determine whether a Windows system is infected with malware. It covers the tools that computer forensics practitioners use to examine a system, build a timeline of events and preserve the state of the system or data they are examining. Common malware attachment points in the Windows operating system are also described.

Learning Objectives
After completing this course, learners should be able to:

- Describe processes and tools used for the preservation of evidence
- Create and preserve disk images
- Understand common methods of malware infection
- Describe basic file system analysis
- Understand general investigative techniques
- Describe malware artifacts on the Windows OS

Who Should Attend
Any FireEye customer.

Technical Requirements
This course includes animation with audio narration and requires Adobe Flash Player and speakers or headphones.
Course Outline

1. Initial Incident Response Processes and Preservation of Evidence
2. Preserving Memory
3. Creating and Preserving Disk Images
4. Common Methods of Malware
5. Investigative Techniques
6. Reporting

For more details, or to view our full course catalog, please visit https://www.fireeye.com/services/training/